



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/642,499	08/18/2003	Matthias Vogel	13906-138001 / 2003P00546	1706
32864 7590 05/01/2007 FISH & RICHARDSON, P.C. PO BOX 1022 MINNEAPOLIS, MN 55440-1022			EXAMINER HOMAYOUNMEHR, FARID	
			ART UNIT 2132	PAPER NUMBER
			MAIL DATE 05/01/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/642,499	Applicant(s) VOGEL ET AL.	
	Examiner Farid Homayounmehr	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 08 February 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-31 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-31 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This action is responsive to communications: application, filed 8/18/2003; amendment filed 2/8/2007.
2. Claims 1-31 are pending in the case.

Information Disclosure Statement PTO-1449

3. The Information Disclosure Statement submitted by applicant on 2/8/200 has been considered. Please see attached PTO-1449.

Response to Arguments

4. Rejection under section 101 is withdrawn due to amendments by the applicant.
5. With regards to rejection based on prior art, applicant describes a summary of their invention and cites several portions of Griffin, the cited reference in the first office action. Applicant further argues: "Griffin does not describe or suggest comparing an access control group identified by the identified user access data entry with an access control group identified by the identified data object access entry and enabling the indicated user to access the indicated data object conditioned on the access control group identified by the identified user

Art Unit: 2132

access data entry being the same access control group as the access control group identified by the identified data object access data entry". However, the mentioned new limitation is disclosed by the search and match operations of a database management system, used as part of the Role Based Access Control System (RBAC), which is suggested in Griffin's paragraph 6. Based on portion of paragraph 6:

"In an administrative system that uses role-based access control, the administrator can be summarized in the following manner: define each role; define the capabilities of the role with respect to resources; connect users to one or more roles; and connect resources to one or more capabilities."

To perform access control, an RBAC system determines the role of a user by searching a database (see parag. 60 or 25 where the use of databases or LDAP is suggested for storage and search of data objects), determines the capabilities of a resource, and determines if the determined role matches with the determined capability. Note that the user role represents user access control group, and capabilities represents data object access control group.

Therefore, the mentioned limitations are disclosed by database search and match operations of database management system used in the RBAC system taught by Griffin (also see the rejection of claim 16 in the next section).

Applicant's argument relative to the new limitations added to claims 25 and 16 is substantially the same as their argument relative to amended claim 1. Note that claim

Art Unit: 2132

16 includes determination of a characteristic for the user and a characteristic for the data object, which is disclosed by Griffin role filters and capability filters (for example, parag. 10 and 11). The role filters and capability filters determine if a role should be matched (access allowed) with a capability based on the characteristics of users or objects (employee title, organization, job status or project assignment, as shown in parag. 10), and automatically generate access rules (parag. 65). Also note that claim 16 includes finding a method to determine the characteristics. The method to determine the characteristics is determined by an additional layer of identifying and linking the entries in tables of a database. Identifying and locating a certain data by linking entries in multiple tables of a database is the main purpose of Relational database systems, and were well known in the art at the time of invention.

Based on the above discussion, applicant's argument relative to allowability of independent claims is found non persuasive. Accordingly, applicant's argument relative to dependent claims is also found non persuasive.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1-31 rejected under 35 U.S.C. 103(a) as being unpatentable over applicants' admitted prior art, Griffin (US Patent Application Publication No. 2002/0178119, filed May 24, 2001).

7.1 As per claim 1, Griffin is directed to a computer-readable storage medium comprising: a data repository Griffin is directed to a system for using databases (parag. 2), which are stored in storage system (parag 19 and Fig. 1A)) including: access control group data including access group entries, an access group entry identifying an access control group (Griffin teaches a role-based access control system (parag. 37), which performs access control using roles (item 302) and capabilities (item 304), as described in parag. 31, 32 and 38. Capabilities 304 identifies access control rules (parag. 38) in a database); user access data including user access data entries (principal 310 as described in parag 38 and 39) a user access data entry relating to at least one entry in the access control group data and identifying a user and an access control group (per paragraph 38, each role is assigned to one or multiple principals. The database of principals is related to roles, which is a set of capabilities (parag. 38), and therefore principals are related to capabilities); and data object access data (resource 306) including data object access data entries, a data object access data entry relating to at least one entry in the access control group data and identifying a data object and access control group (per paragraph 41, capabilities define access rules to resources, therefore resources are related to capabilities); and executable instructions that when executed perform operations comprising:

Art Unit: 2132

receiving an indication of a user (Griffin teaches Role Based Access Control (RBAC) systems in parag. 6, which shows a user is connected to a role. Griffin also teaches sing LDAP and databases to store and search for data objects (see parag. 60 or 25). It is known in the art that RBAC systems search database tables to find a match for the user to associate it with a role. Database systems search tables to find a match of an entered data item (see the attached copy of definition of Database Management systems from Wikipedia), and link tables based on the common entries to search and located other information related to the data entry);

receiving an indication of a data object (parag. 6 shows resources (data objects) are connected to capabilities);

searching the user access data to identify a user access data entry that identifies the indicated user (as mentioned above, the role of a user is determined by searching the database table representing user data);

searching data object access data to identify a data object access data entry that identifies the data object (as mentioned above, the capabilities associated with a resource is determined by searching the database table representing the resource);

comparing an access control group identified by the identified user access data entry with an access control group identified by the identified data object access entry (compare the capabilities of a role with capabilities associated to resources, as shown in parag. 6);

enabling the indicated user to access the indicated data object conditioned on the access control identified by the identified user access data entry being the same

Art Unit: 2132

access control group as the access control group identified by the identified data object access data entry (It is well known that an RBAC system allows access when the capabilities of the role associated with a user matches the capabilities associated with a resource).

7.2. As per claims 2, 3 and 4, Griffin is directed to the medium of claim 1 wherein at least one entry in the access control group data includes a characteristic for use in determining at least one entry in the user access data or in the data object access data that relates to the at least one entry in the access control group data structure (as indicated in Fig. 3 and associated text, Griffin teaches role and capability filters that associate characteristics of user data or resources to roles and capabilities (see parag. 40-46). Based on the attributes of principals and resources, filters associate a role or a resource to a capability).

7.3. As per claims 5, 6, and 7, Griffin is directed to the medium of claim 1 wherein at least one entry in the access control group data includes an indication of an access control rule for use in determining: at least one entry in the user access data structure that relates to the at least one entry in the access control group data, and at least one entry in the data object data that relates to the at least one entry in the access control group data structure (as mentioned in response to claims 2-4, filters relate a characteristic to relate an entry in resource/principal (data/user) databases to an entry

in capabilities (access control group) database. The filters use an indication of a relationship between entries of databases to make a connection).

7.4. As per claim 8, Griffin is directed to the medium of claim 1 wherein the data repository further includes access rule data including access rule entries, an access control rule entry relating to at least one entry in the access control group data (Griffin's capabilities include access rules to determine if access to a specific resource is allowed for a specific principal (user)).

7.5. As per claims 9, Griffin is directed to the medium claim 8 wherein at least one entry in the access rule data includes an indication of action that is permitted to be performed for at least one entry in the data object access data (capabilities include an indication of an action that is permitted to be performed to a resource).

7.6. As per claim 10, Griffin is directed to the medium of claim 8 wherein at least one entry in the access rule data includes an indication of how to determine at least one entry in the data object access data that relates to at least one entry in the access control group data (rule data structure is part of Griffin's capabilities data structure, which per response to claims 5-7 an indication to determine how one entry in the data object access data structure relates to one entry in the capabilities data base).

7.7. As per claim 11, Griffin is directed to the medium of claim 8 wherein at least one entry in the access rule data structure includes an indication of how to determine at least one entry in the user access data that relates to at least one entry in the access control group data (rule data structure is part of Griffin's capabilities data structure, which per response to claims 5-7 an indication to determine how one entry in the user access data structure relates to one entry in the capabilities data base).

7.8. As per claim 12, Griffin is directed to the medium of claim 1 wherein each of the access control group data structure, the user access data, and the data object access data structure are each separately maintainable from each of the other data (parag. 35 shows each data structure can be configured independently from the others, and relationships established by filters).

7.9. As per claim 13, Griffin is directed to the medium of claim 1 wherein each of the user access data structure and the data object access data are separately maintainable from the other data structure (see response to claim 12).

7.10. As per claim 14, Griffin is directed to the medium of claim 13 wherein a change in the user access data does not necessitate a change in the data object access data to maintain desired control over access by particular users to particular data objects (see response to claim 13. As the databases are independent from one another, change in one does not necessitate change in other).

7.11. As per claim 15, Griffin is directed to the medium of claim 13 wherein a change in the data object access data does not necessitate a change in the user access data to maintain desired control over access by particular users to particular data objects (see response to claim 14).

7.12. Limitations of claim 16 are substantially the same as limitations of claim 1. Note that the capabilities database contains access control rules and resource database contains characteristics data that relates to capabilities data base entries. Also note that filters create association between capabilities and resources based on characteristics of resources, such as the role of a resource (printer manager) or time limits to login as mentioned in parag. 41. Furthermore, claim 16 includes searching database tables, and identifying a method to determine characteristics, which is just another layer of searching and linking on the items stored on a database management system. Griffin teaches addition of a new layer of abstraction (see parag. 7, where the addition of roles is taught) to improve scalability, auditability and quality. It would have been obvious to a person skilled in art to add additional layers, such as a database table to define a method to determine characteristics of the user or data objects.

7.13. As per claim 17, Griffin is directed to the medium of claim 16 further comprising a user data to store user data (principal 310 as described in claim 1).

Art Unit: 2132

7.14. As per claim 18, Griffin is directed to the medium of claim 17 wherein at least one entry in the characteristic method data structure includes an indication of a method to determine a user characteristic associated with at least one entry in the user data (As mentioned in response to claim 16, it would have been obvious to add additional layers, such as describing a method to determine the characteristic of the user or data object).

7.15 As per claim 20, Griffin is directed to the medium or propagated signal of claim 18 wherein at least one entry in the characteristic method data structure includes an indication of a criterion for use in eliminating at least one entry in the data object data structure when using the method to determine a user characteristic (parag. 48 shows active role processing examines deletion of entries in the resource data structure, and runs filters to reflect the changes (deletion) in other databases, therefore there is an indication of deletion of entries in resource database in the roles database)

7.16. Limitations of claims 19, 21-26 are substantially the same as limitations of claims 1-18 and 20 above.

7.17. As per claims 27 and 28, it would have been obvious to a person skilled in art to use the same method to determine the characteristics of the user and the characteristics of the data object, or use different methods to determine the characteristics of the user and the characteristics of the data object.

7.18. As per claim 29, Griffin paragraphs 31 and 32 indicate that each user may be assigned several roles, and each role may be assigned several capabilities. Therefore Griffin teaches multiple entries for the access control rules for each user or role.

7.19. As per claims 30 and 31, Griffin teaches the characteristic data includes a first characteristic method data entry identifying a first method to determine a characteristic for a user and a second characteristic method data entry identifying a second method to determine a characteristic for a user, the first and second method being the same or different (see response to claims 27-29).

Conclusion

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

Art Unit: 2132

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

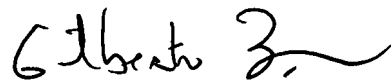
9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is (571) 272-3739. The examiner can be normally reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Farid Homayounmehr

4/27/2006


GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100